UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/660,370	09/12/2000	Thomas P. Hardjono	120-244	6652

34845 7590 09/26/2007
McGUINNESS & MANARAS LLP
125 NAGOG PARK
ACTON, MA 01720

EXAMINER	
TRAN, TONGOC	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
09/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/660,370	HARDJONO, THOMAS P.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-12,18-21,26-36 and 48-65* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-12,18-21,26-36 and 48-65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to Applicant's amendment filed on July 2, 2007. Claims 1, 18, 20, 26, 29 and 32 have been amended. Claims 2, 4, 13-17, 22-25, 37-47and 66-69 have been previously canceled. Claims 1, 3, 5-12, 18-21, 26-36 and 48-65 are pending.

Response to Arguments

2. Applicant's arguments with respect to independent claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3, 5-12, 18-21, 26-36 and 48-65 rejected under 35 U.S.C. 103(a) as being unpatentable over Ballardie ("Scalable Multicast Key Distribution ", Network Working Group, Univesity College London, 1996) in view of Bird et al. ("The KryptoKnight Family of Light-Weight Protocol for Authentication and Key Distribution", IEEE/ACM Transactions on Networking, Vol. 3, No. 1 February 1995, B. Two-Way Authentication –Basic Building Block, pages 32-33, hereinafter Bird) and further in view of Mittra S. ("Iolus: A Framework for Scalable Secure Mutlicasting", ACM 1997).

In respect to claim 1, Ballardie discloses a communication system comprising:

a rendezvous point device that forwards multicast communication messages to members of a shared tree; a designated device in communication with the rendezvous point device via a number of intermediate devices (see pages 8-12, e.g. host h, router A and B-intermediate device and Core router-rendezvous point device, page 11);

a host device in communication with a designated device, wherein: the host device forwards an authentication key, generated by a key server for the host device, to the designate device (page 10, last paragraph – page 11, first paragraph, page 2, third paragraph, the key server is inherently required in order for the key to be generated).

the host device sends a join request to the designated device using a predetermined multicast group management protocol in order to join the shared tree for receiving the multicast communication messages forwarded by the rendezvous point device (pages 9-11);

the designated device receives the join request and forwards to the rendezvous point device via the number of intermediate devices an encoded join request generated using an authentication key associated with the host device (pages 9-10);

the rendezvous point device receives the encoded joint request and authenticates the encoded join message using the authentication key associated with the host device; and the host device is prevented from receiving the multicast communication messages forwards by the rendezvous point device, if the rendezvous point device determined that the encode join message is not authentic (pages 10, last paragraph-page 12, 3rd paragraph).

Ballardie does not explicitly disclose the encoded join request comprises a tag field computed using a keyed hash function and the authentication key and a nonce field comprising a number for preventing playback attack. However, Bird discloses a protocols for performing a two way authentication with tag field for cryptographic one-way hash functions, a MAC called Message Authentication Codes and a nonce field to prove a network's identity (see Bird, page 32, col. 2, 2nd paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the protocols taught by Bird with the encoded join request of Ballardie to ensure the security of the network is protected and at the same time efficient in message size and computation overhead and resistant to a wide set of attacks (Bird, page 32, col. 2, 1st paragraph). Mittra further discloses the rendezvou point device is a root of the shared tree and authenticates the encoded join request by comparing the authentication key received in the tag against a stored authentication key associated with the host device (e.g. Mittra, page 281-281, "5 The Iolus Framework", "the GSA form a hierarchy of subgroups. The GSC maintains control of the top-level subgroup at the root of the secure distribution tree. It is ultimately responsible for the security of the entire group. GSIs are special trusted servers that are authorized to act as proxies of the GSC or their parent GSIs and control their local subgroup"; "6.1 Startup, The GSC is supplied with an access control list (ACL) that it uses to set the security policy concerning who may have what access to the group"; "6.2 Joins, "the GSA checks its database and decides whether to approve, it (1) generates a secret ($K_{Gsa-MBr}$) to be shared **only** with the new member, (2) stores this secret along with any other relevant

information concerning the new member in a private database it maintains, and then communicate $K_{GSA-MBR}$ to the new member using secure channel". Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of secure joining of multicast communication taught by Ballardie with Mittra's a rendezvous point device being a root of the shared tree that are supplied with an ACL or database to ensure secure joining a multicast group (e.g. Mittras, page 282, Joins). In addition, Examiner asserts that authenticating by identifying a party or device using unique keying information is old and well known. Examiner further asserts that distributing a group key for secure communication after successful authentication of a host is also well known. It would have been obvious to one of ordinary skill in the art to implement the joining process taught by Ballardie or Mittra to ensure the authenticity of the host that is joining the group and subsequence secure multicast group communication.

In respect to claim 3, Ballardie discloses the communication system of claim 1, wherein the key server provides the authentication key to both the host device and the rendezvous point device using a secure key distribution mechanism (pages 8-11).

In respect to claim 7, Ballardie discloses the communication system of claim 1, wherein the designated device joins the shared tree on behalf of the host device (see pages 10-11).

In respect to claim 8, Ballardie discloses the communication system of claim 7, wherein the designated device establishes appropriate multicast routes for forwarding multicast communication messages to the host (see Ballardie, pages 9-12).

In respect to claim 9, Ballardie discloses the communication system of claim 1, wherein each intermediate device receives the encoded join request and forwards the encoded join request toward other routing element (see page 10).

In respect to claim 10, Ballardie discloses the communication system of claim 9, wherein each intermediate device that is not already joined to the shared tree joins the shared tree on behalf of the host device and establishes appropriate multicast routes for forwarding multicast communication messages toward the host device upon receiving the join request (see Ballardie, pages 8-12).

In respect to claim 11, Ballardie discloses the communication system of claim 9, wherein each intermediate device that is already joined to the shared tree waits for an explicit acknowledgment message from the primary router and establishes appropriate multicast routes for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the primary router (see Ballardie, pages 8-12).

In respect to claim 12, Ballardie disclose the communication system of claim 1, wherein the primary router sends an explicit acknowledgment message toward the host device upon determining that the join request is authentic (see Ballardie, page 9-12).

In respect to claim 18, Ballardie discloses a method comprising:

Obtaining an authentication key associated with a host device from a key server following authentication of the host device by the key server; and sending a join request to a designated device using a predetermined multicast group management protocol, the join request including the authentication key for use by the designated device for

encoding the join message prior to forwarding of the join message to rendezvous point (see Ballardie, pages 8-12, page 10, last paragraph – page 11, first paragraph, col. 2, third paragraph, the key server is inherently required in order for the key to be generated).

In respect to claim 19, the claim limitation is similar to claim 6. Therefore, claim 19 is rejected based on the similar rationale.

In respect to claims 20-21, the claim limitations are similar to claims 18-19. Therefore, claims 20-21 are rejected based on the similar rationale.

In respect to claim 26, Ballardie discloses a method comprising:

Receiving a join request from a host device; generating an encoded join request using an authentication key associated with the host device; and sending the encoded join request toward a rendezvous point device to enable authentication of the join message at the rendezvous point using the authentication key associated with the host device (see Ballardie, pages 8-12; page 2, third paragraph).

Ballardie does not explicitly disclose the encoded join request comprises a tag field computed using a keyed hash function and the authentication key and a nonce field comprising a number for preventing playback attack. However, Bird discloses a protocols for performing a two way authentication with tag field for cryptographic one-way hash functions, a MAC called Message Authentication Codes and a nonce field to prove a network's identity (see Bird, page 32, col. 2, 2nd paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the protocols taught by Bird with the encoded join request of Ballardie to

ensure the security of the network is protected and at the same time efficient in message size and computation overhead and resistant to a wide set of attacks (Bird, page 32, col. 2, 1st paragraph).

In respect to claim 27, Ballardie discloses the method of claim 26, wherein the join request includes the authentication key (see Ballardie, page 10).

In respect to claim 28, Ballardie discloses the method of claim 26, further comprising:

Joining a shared tree on behalf of the host device and establishing and establishing appropriate multicast routes for forwarding multicast communication messages to the host devices (see Ballardie, pages 8-12).

In respect to claims 29-36, the claim limitations are similar to claims 26-28. Therefore, claims 29-36 are rejected based on the similar rationale.

In respect to claim 48, Ballardie discloses a method comprising:

Receiving, from a designated routing device coupled to a host an encoded join request for the host device, the encoded join request being encoded by the designated routing device using an authentication key associated with the host, the authentication key being received by the host device following authentication of the host device by a key server and forwarded in a join request forwarded from host device to the designed routing device; the authentication key being received by the host device following authentication of the host device by a key server and forwarding in a join request forwarded from host device to the designed routing device (see Ballardie, pages 8-12, note page 10, last paragraph – page 11, first paragraph, page 2, third paragraph, the

key server is inherently required in order for the key to be generated and distributed); authenticating the encoded join request using the host device authentication key to determine whether or not the encoded joint message is authentic; and establishing appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the join request is determined to be authentic (see Ballardie, pages 8-12, page, e.g. "c also authenticates host h", page 10, last paragraph to page 12, third paragraph; page 2, third paragraph).

Ballardie does not explicitly disclose the encoded join request comprises a tag field computed using a keyed hash function and the authentication key and a nonce field comprising a number for preventing playback attack. However, Bird discloses a protocol for performing a two-way authentication with tag field for cryptographic one-way hash functions, a MAC called Message Authentication Codes and a nonce field to prove a network's identity (see Bird, page 32, col. 2, 2nd paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the protocols taught by Bird with the encoded join request of Ballardie to ensure the security of the network is protected and at the same time efficient in message size and computation overhead and resistant to a wide set of attacks (Bird, page 32, col. 2, 1st paragraph).

In respect to claim 49, Ballardie discloses the method of claim 48, wherein authenticating the encoded join request comprises:

maintaining a number of authentication keys; determining the host device for the encoded join request; and searching for an authentication key associated with the host device (see Ballardie, page 10, last paragraph to page 12, third paragraph).

In respect to claim 50, Ballardie discloses the method of claim 49, wherein authenticating the encoded join request further comprises:

failing to find an authentication key associated with the host device; and determining that the encoded ,loin request is not authentic (see Ballardie, page 10, last paragraph to page 12, third paragraph).

In respect to claim 51, Ballardie discloses the method of claim 49, wherein authenticating the encoded join request further comprises:

finding an authentication key associated with the host device; and authenticating the encoded join request using the authentication key associated with the host device (see Ballardie, page 10, last paragraph to page 12, third paragraph).

In respect to claim 52, Ballardie discloses the method of claim 48, further comprising:

sending an explicit acknowledgment toward the host device if and only if the encoded join request is determined to be authentic (see Ballardie, page 10, last paragraph to page 12, third paragraph).

In respect to claims 53-62 and 65, the claim limitations are apparatus and computer readable medium and a communication system claims that are substantially similar to method claims 48-52. Therefore, claims 53-62 and 65 are rejected based on the similar rationale.

In respect to claims 63-64, Ballardie discloses the computer readable medium of claim 58, wherein the computer readable medium is a computer storage medium and a communication medium (see Ballardie, page 1).

In respect to claim 65, the claim limitation is substantially similar to claim 1. Therefore, claim 65 is rejected based on the similar rationale.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

September 17, 2007

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER